

PENDEKATAN STEGO-KRIPTO MODE CIPHER BLOCK CHAINING UNTUK PENGAMANAN INFORMASI PADA CITRA DIGITAL

Vera Wati¹; Hanifat Sa'diyah²; Dony Ariyus³

Magister Teknik Informatika¹²³
Universitas AMIKOM Yogyakarta
www.mti.amikom.ac.id

verave.wati@gmail.com¹; hanifputri2013@gmail.com²; dony.a@amikom.ac.id³

Abstract— Digital image can be one of the media for information security. The contents of information have an important value of effectiveness, one of which is as a support in decision making. Then the information needs to be done to safeguard the authority of parties who are not responsible. Such security can utilize Steganography and Cryptography (Stego-Crypto). The method used combines Stego-Crypto by randomizing information using Cipher Block Chaining (CBC) then the encryption results are secured through digital images. Based on the test results by measuring the capacity of information on the image produces test data if CBC can process characters in uppercase, spaces and other characters and the results of plaintext and ciphertext produce a ratio of 1: 2, but the LSB performance only accommodates characters depending on the number of sizes on digital image. Testing by evaluating the difference in pixel histogram, when viewed with an invisible not very visible difference, but the insertion of messages with 100-200 characters causes the addition of the average image size on stego images larger than 1: 4, the value of 1 from the original image. Besides, testing with the help of communication media, stego images or encrypted images is able to use email to send stego images because LSB is sensitive to the process of resizing images.

Keywords: Stego-Crypto, CBC, Information Security, LSB.

Intisari— Citra Digital bisa menjadi salah satu media untuk pengamanan informasi. Isi pada sebuah informasi memiliki nilai efektivitas yang penting, salah satunya sebagai penunjang dalam pengambilan keputusan. Maka informasi perlu dilakukan pengamanan untuk mencegah wewenang dari pihak yang tidak bertanggung jawab. Pengamanan tersebut bisa memanfaatkan Steganografi dan Kriptografi (Stego-Kripto). Metode yang digunakan mengkombinasikan Stego-Kripto dengan mengacak informasi menggunakan Cipher Block Chaining (CBC) kemudian hasil enkripsi tersebut diamankan melalui citra digital. Berdasarkan hasil pengujian dengan mengukur kapasitas informasi pada citra menghasilkan data uji jika CBC dapat memproses karakter berupa huruf

besar-kecil, spasi dan karakter lainnya dan hasil plainteks dan cipherteks menghasilkan perbandingan jumlah 1:2, namun kinerja LSB hanya menampung karakter bergantung pada jumlah ukuran pada citra digital. Pengujian dengan evaluasi perbedaan pixel histogram, jika dilihat dengan kasatmata tidak terlalu nampak perbedaannya, namun penyisipan pesan dengan 100-200 karakter menyebabkan penambahan ukuran gambar rata-rata pada citra stego lebih besar 1:4, nilai 1 dari citra asli. Selain itu, pengujian dengan bantuan media komunikasi, citra stego atau citra yang terenkripsi mampu memanfaatkan email untuk mengirimkan citra stego karena LSB sensitif pada proses pengubahan ukuran citra.

Kata Kunci: Stego-Kripto, CBC, Pengamanan Informasi, LSB.

PENDAHULUAN

Citra digital adalah representatif yang menggambarkan bentuk dari imitasi pada objek sehingga memiliki kemiripan (Darma, 2010). Citra bisa menjadi salah satu alternatif media pengamanan informasi, dimana secara cepat kasat mata manusia tidak akan menyadari jika terdapat informasi rahasia didalamnya. Melalui teknik kriptografi untuk mengamankan informasi dengan mengacak pesan asli menjadi pesan tersandi kemudian digunakan teknik Steganografi sebagai media penyimpanan informasi tersebut, sehingga mendapatkan keamanan tertinggi.

Penelitian oleh (Saleh, 2009) memanfaatkan metode Cipher Block Chaining (CBC) dan Least Significant Bit (LSB) mampu meningkatkan keamanan data, ketika teknik kriptografi dengan CBC menjamin tidak ada duplikasi pada blok tiap proses enkripsi. Steganografi dengan 4LSB yang dilakukan peneliti (Jawed & Das, 2015) memiliki tingkat keamanan yang dapat dipulihkan dan dicurigai pihak ketiga dan penelitian tersebut juga memanfaatkan metode Stego Block Chaining (SBC) hanya meningkatkan keamanan sementara dan jumlah iterasi harus selalu dirahasiakan.

Metode lain dengan kombinasi Hill Cipher dan LSB yang dimanfaatkan dalam penelitian

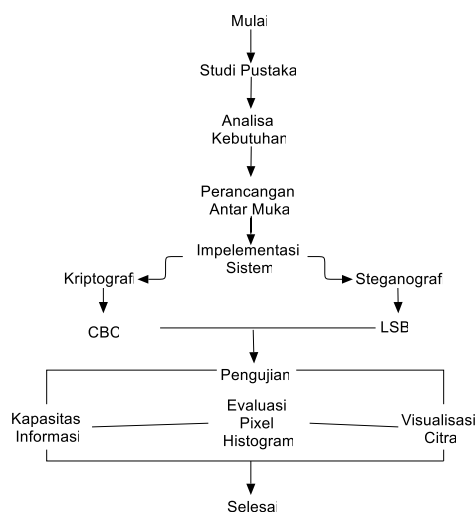


(Hermansa, Umar, & Yudhana, 2019), jika proses steganografi dengan LSB menghasilkan informasi pada citra digital aman dan tidak diketahui oleh kasat mata. Teknik Steganografi dengan LSB dalam penelitian (Hernawandra, Supriyadi, & Lenggana, 2018) mampu terkombinasikan dengan Vigenere hanya mengevaluasi penambahan rata-rata ukuran citra asli dengan citra stego, lain hal dengan penelitian serupa oleh (Syawal, Fikriansyah, & Agani, 2016) masih ada keterbatasan tidak dapat menginputkan huruf kecil dan spasi.

Maka dalam penelitian ini melakukan kombinasi kriptografi Cipher Block Chaining (CBC) yang mampu mengenkripsi informasi rahasia dengan berbagai macam karakter kemudian disembunyikan pada citra digital berbasis Least Significant Bit (LSB) dimana pesan disisipi pada bit terakhir. Hal tersebut untuk menguji ketahanan informasi yang tersimpan pada citra digital dengan pendekatan Stego-Kripto. Sehingga meningkatkan keamanan isi informasi tanpa dicurigai penyerang.

BAHAN DAN METODE

Penelitian ini menggunakan 2 (dua) metode dalam pengamanan informasi, yaitu menggunakan Kriptografi dalam menjaga kerahasiaan informasi dengan seni perhitungan matematika dalam pengubahan pesan terbaca menjadi tidak bermakna yang dikenal dengan enkripsi (Ariyus, 2008). Metode lain, yakni Steganografi dimana informasi yang telah terenkripsi disisipkan pada citra digital sehingga informasi tersamarkan meminimalisir kecurigaan pihak ketiga (Sari, Sulindawaty, & Sihotang, 2017). Proses ini dilibatkan dalam pengimplementasian sistem. Tahapan penelitian Stego-Kripto Mode CBC terdapat pada Gambar1.



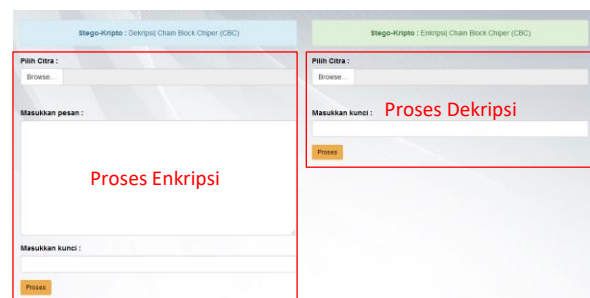
Sumber: (Wati, Sa'diyah, & Ariyus, 2019)
Gambar1. Alur Penelitian Stego-Kripto Mode CBC untuk Pengamanan Informasi pada Citra

Pada Gambar 1. sebelum dilakukan implementasi sistem, tahap yang dilakukan adalah analisa kebutuhan meliputi teks dan citra digital yang akan digunakan dalam pengujian selain itu kebutuhan hardware dan software yang berkaitan demi keberlangsungan penelitian. Kebutuhan hardware meliputi laptop dan beberapa kebutuhan software Xampp Control Panel, bahasa Pemrograman PHP menggunakan teks editor dengan Sublime Text 3 dan web browsernya. Perancangan antarmuka mempermudah penggunaan sistem saling berkomunikasi dengan user (Arta, 2017). Tahapan pengimplementasian dilakukan dengan proses Kriptografi dengan metode CBC dan Steganografi memanfaatkan LSB, kemudian akan dilakukan pengujian.

Pentingnya pengujian dilakukan untuk memastikan jika hasil keluaran sistem berhasil sesuai kebutuhan (Sari, dkk., 2017). Pengujian dengan penyisipan kapasitas informasi untuk mengetahui daya tampung penyisipan informasi dengan jumlah dan berbagai karakter citra digital, evaluasi pixel histogram yaitu dengan mengevaluasi perbedaan dari citra asli dibandingkan dengan citra stego dan pengujian dengan visualisasi citra yaitu dengan melihat perbedaan dengan menggunakan media komunikasi dan pengiriman citra untuk mengetahui ketahanan pesan informasi pada citra.

HASIL DAN PEMBAHASAN

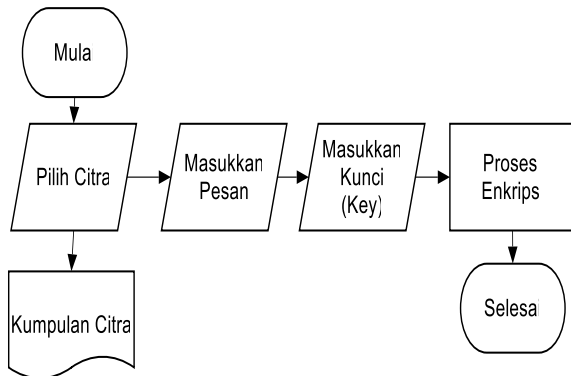
Tahapan pada pengimplementasian dilakukan dengan metode Kriptografi dan Steganografi yang melibatkan proses enkripsi dan dekripsi. Antarmuka pada Stego-Kripto mode CBC lihat pada Gambar1.



Sumber: (Wati, Sa'diyah, & Ariyus, 2019)
Gambar2. Rancangan Antarmuka Proses Enkripsi dan Dekripsi Stego-Kripto Pengamanan Informasi

1. Proses Enkripsi

Proses enkripsi adalah proses pengubahan pesan terbaca (plainteks) menjadi pesan acak (cipherteks) (Azmi & Erika, 2017), (Fadlan & Hadriansa, 2017). Ilustrasi pada Gambar3.



Sumber: (Wati, Sa'diyah, & Ariyus, 2019)

Gambar 3. Alur Proses Enkripsi Stego-Kripto Mode CBC

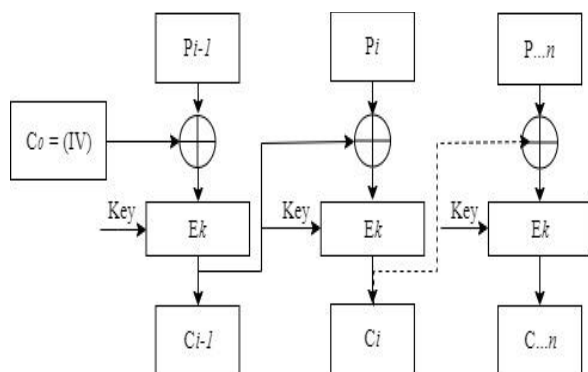
Pada Gambar3. untuk proses enkripsi diawali dengan pengambilan citra kemudian akan dimasukkan informasi dan masukkan *key*. Proses Enkripsi melibatkan metode CBC dengan persamaan (1)(2)(3)

$$C_0 = E_k (P_0 \oplus IV), C_0 = IV \dots \dots \dots (1)$$

$$C_i = E_k (P_i \oplus C_{i-1}) \dots \dots \dots (2)$$

$$C_{\dots n} = E_k (P_{\dots n} \oplus C_{\dots n}) \dots \dots \dots (3)$$

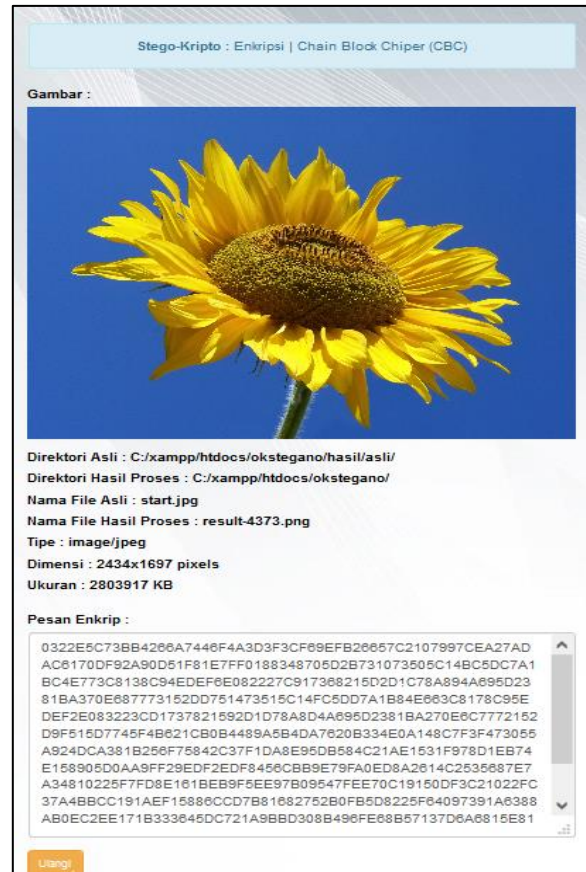
Dimana, nilai pada C_i nilai i mewakili indeks pada pesan yang akan terenkripsi dari nilai i sampai nilai n . Pada nilai C_0 dimana 0 mewakili nilai dari IV yaitu nilai Insialisasi Vector (IV). Nilai IV termanfaatkan dalam penelitian sebagai pengoperasian yang di inisiasi awal pada block (Saleh, 2009). Metode CBC merupakan salah satu metode kriptografi dengan model sekuensial mode operasi block cipher (Rochmah & Ardiansyah, 2016). Mekanisme pada CBC menerapkan *feedback* pada hasil block sebelumnya. Skema CBC pada proses enkripsi lihat pada Gambar4.



Sumber: (Wati, Sa'diyah, & Ariyus, 2019)

Gambar4. Skema Enkripsi Operasi Mode CBC

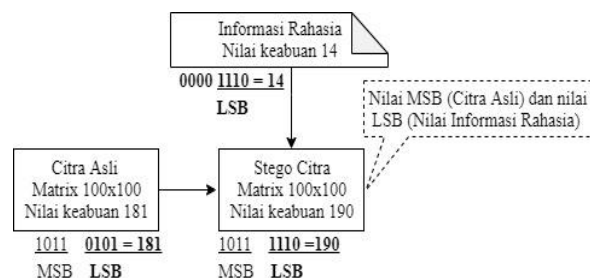
Keistimewaan pada mode CBC terdapat pada nilai IV, karena membuat tiap blok hasil enkripsi menjadi blok acak dan unik (Zebua, 2015).



Sumber: (Wati, Sa'diyah, & Ariyus, 2019)

Gambar5. Rancangan Antarmuka Proses Enkripsi

Dijelaskan pada rancangan antarmuka Gambar 5. tipe file dengan jpeg, dengan dimensi 2434x1697 pixels dan ukuran 2803917 KB dalam bentuk Biner, mampu menyisipkan informasi sehingga mampu menampilkan pesan enkripsi. Pada teknik Steganografi, untuk penyisipan informasi peneliti menggunakan metode Least Bit Significant (LSB) dengan melakukan pengubahan bit yang memiliki nilai *redundancy* pada citra yang akan disisipi informasi, sehingga citra menyerupai seperti semula (Jawed & Das, 2015) (Danuputri, Mantoro, & Hardjianto, 2016). Gambaran pengubahan citra memiliki nilai 8 bit berbasis pixel, dibagi menjadi 4 bit MSB dan 4 bit LSB seperti ditunjukkan pada Gambar4.



Sumber: (Wati, Sa'diyah, & Ariyus, 2019)

Gambar4. Mekanisme Least Significant Bit (LSB)



Sesuai Gambar4. kinerja dari LSB bertugas menyisipkan informasi rahasia, namun nilai keabuan piksel pada 4 bit awal Most Significant Bit (MSB) dan 4 bit akhir nilai LSB (Cheddad, Condell, Curran, & Mc Kevitt, 2010). Selain itu, LSB dikenal memiliki hasil dengan nilai transparansi yang tinggi (Jain, 2019). Teknik Steganografi tidak melakukan pengubahan warna secara signifikan, misalkan pada sebuah citra terdapat nilai-nilai piksel Red, Green, Blue (RGB) berikut :

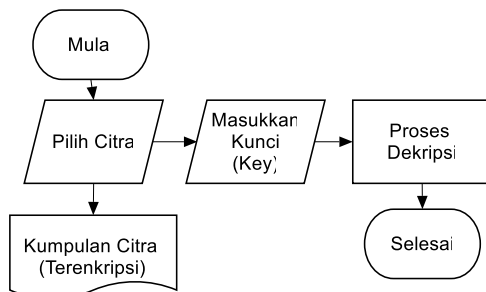
R	G	B
11010011	10101010	11100011
01001001	00010010	10101111
11111100	11000011	10101000

Kemudian akan disisipi informasi rahasia dengan nilai bit 11100110, maka akan mengganti bit terakhir pada citra asli, dengan hasil citra stego;

R	G	B
1101001 <u>1</u>	1010101 <u>1</u>	1110001 <u>1</u>
0100100 <u>0</u>	0001001 <u>0</u>	1010111 <u>1</u>
1111110 <u>1</u>	1100001 <u>0</u>	1010100 <u>0</u>

2. Proses Dekripsi

Proses Dekripsi merupakan proses pengembalian pesan tidak bermakna (cipherteks) menjadi pengubahan pesan terbaca (plainteks). Pengubahan informasi ke semula di ilustrasikan pada Gambar6.



Sumber:(Wati, Sa'diyah, & Ariyus, 2019)

Gambar 6. Alur Proses Dekripsi Stego-Kripto Mode CBC

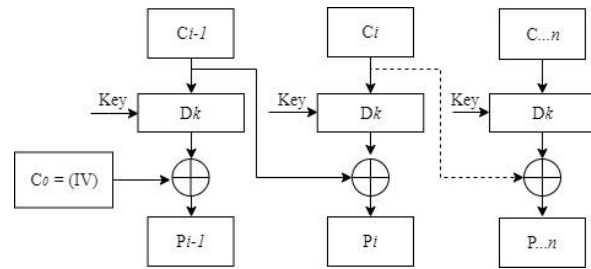
Proses Dekripsi pada penggunaan Cipher Block Chaining (CBC), memilih citra yang sudah tersisipi pesan kemudian masukkan kunci, kemudian diproses (seperti Gambar6.). Fungsi matematis dekripsi operasi mode CBC sebagai berikut (4)(5)(6)

$$P_0 = D_k (C_0) \oplus C_{i-1}, C_0 = IV \dots\dots\dots(4)$$

$$P_i = D_k (C_i) \oplus C_{i-1} \dots\dots\dots(5)$$

$$P \dots n = D_k (C) \dots n \oplus C \dots n) \dots\dots\dots(6)$$

Nilai pada Dekripsi mengubah nilai Cipherteks ($C_{i..n}$) menjadi Plainteks ($P_{i..n}$). Dijelaskan pada Skema Dekripsi tertera pada Gambar 7.

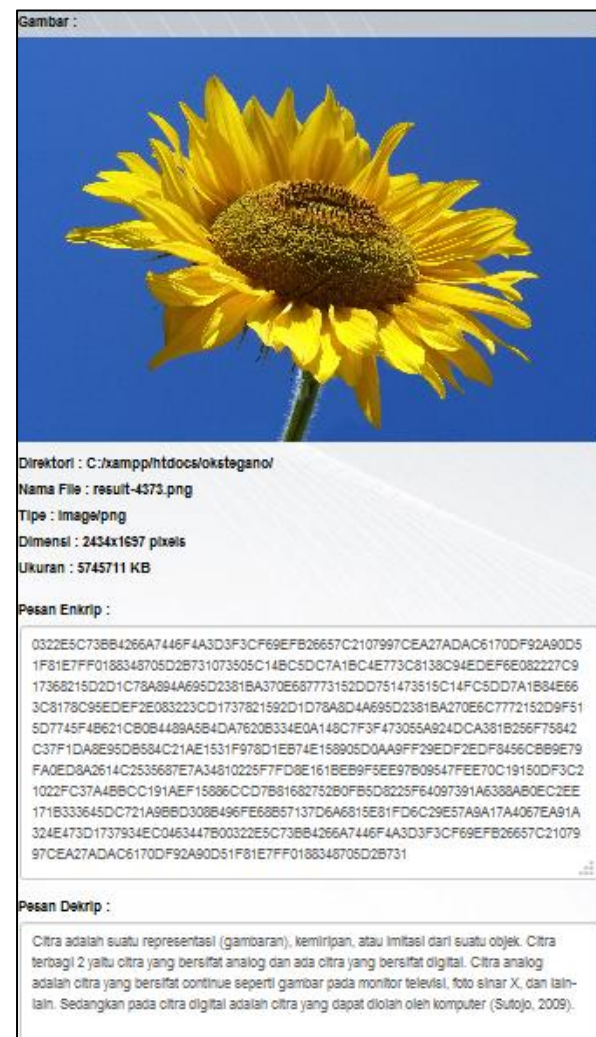


Sumber: (Wati, Sa'diyah, & Ariyus, 2019)

Gambar 7. Skema Dekripsi Operasi Mode CBC

Penerapan Dekripsi mode CBC akan menghasilkan deskripsi citra dengan sedikit perbedaan, yaitu menghasilkan tipe .png, dimensi 2434x1697 pixels dan resolusi sebesar 5745711 KB seperti pada Gambar8.

Sesuai Gambar8 pada citra maka nilai LSB pada citra tersebut maka representasi citra akan menampilkan pesan yang telah tersisipi. Perubahan ini tidak akan terlalu disadari oleh kasat mata (Cahyadi, 2012).



Sumber:(Wati, Sa'diyah, & Ariyus, 2019)

Gambar 8. Rancangan Antarmuka Proses Dekripsi

Pada Gambar8. Rancangan antarmuka kinerja CBC ketika proses dekripsi mampu mengembalikan pesan teks kebentuk semula, walaupun plainteks beragam karakter seperti spasi, huruf besar kecil, tanda baca dan angka. Proses tersebut menggunakan kunci dengan kombinasi karakter yaitu "Kriptografi 2019:*".

Beberapa pengujian telah digunakan dalam penelitian, diantaranya :

1. Pengamanan Kapasitas Informasi

Pada pengujian ini menggunakan plainteks dengan panjang karakter secara bertingkat, sehingga mendapatkan hasil sesuai pada Tabel 1.

Tabel1. Pengujian Kapasitas Informasi

Deskripsi Citra Asli	Jumlah Karakter		Deskripsi Citra Stego	Keberhasilan	
	P	C		Enkripsi	Dekripsi
image/jpeg, 4160x3120 pixels, 1086976 KB	50	100	image/png, 4160x3120 pixels, 2037966 KB	✓	✓
image/jpeg, 4160x3120 pixels, 1086976 KB	100	200	image/png, 4160x3120 pixels, 2037966 KB	✓	✓
Image/jpeg, 4160x3120, pixels, 1086976 KB	200	-	-	✓	✗
Image/jpeg, 4160x3120 pixels, 1086976 KB	300	-	-	✓	✗
image/jpeg, 4160x3120 pixels, 1086976 KB	400	-	-	✓	✗
Citra dengan ukuran + 2000000 KB (dalam KB biner)					
Image/jpeg, 2434x1697 pixels, 2803917 KB	50	100	image/png, 2434x1697 pixels, 5745535 KB	✓	✓
Image/jpeg, 2434x1697 pixels, 2803917 KB	100	200	image/png, 2434x1697 pixels, 5745535 KB	✓	✓
Image/jpeg, 2434x1697 pixels, 2803917 KB	300	600	image/png, 2434x1697 pixels, 5745711 KB	✓	✓
Image/jpeg, 2434x1697 pixels, 2803917 KB	400	800	image/png, 2434x1697 pixels, 5745778 KB	✓	✓
Image/jpeg, 2434x1697 pixels, 2803917 KB	500	1000	image/png, 2434x1697 pixels, 5745835 KB	✓	✓

Sumber:(Wati, Sa'diyah, & Ariyus, 2019)

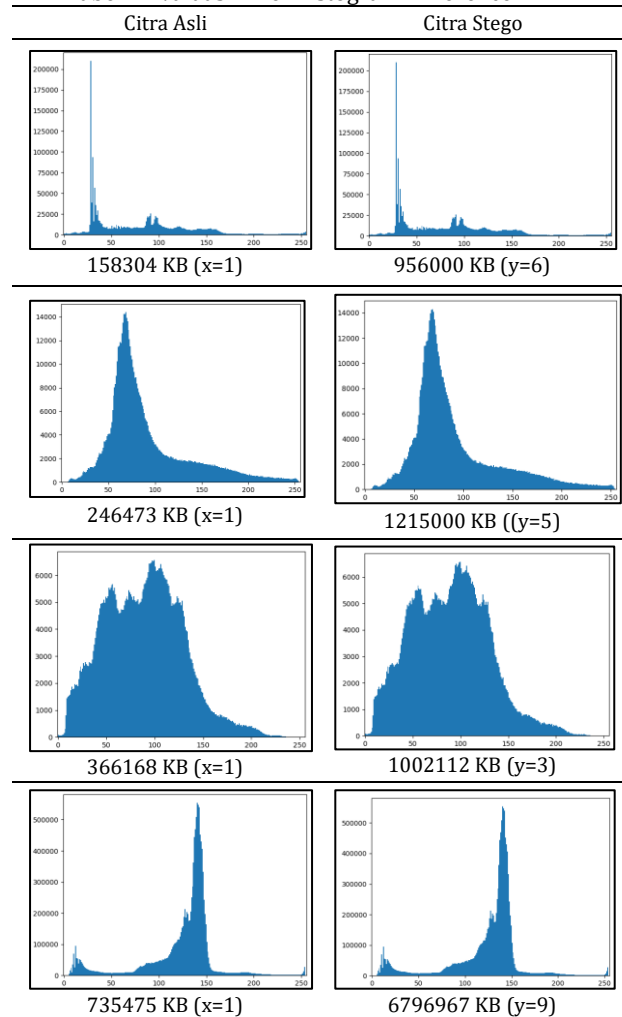
Pada pengujian penyisipan kapasitas sesuai Tabel1., jika 'P' mewakili Plainteks 50 karakter (berserta spasi) maka hasil 'C' mewakili Cipherteks sejumlah 100 karakter. Hal demikian dikarenakan mode CBC dimodifikasi hasil enkripsi ditampung

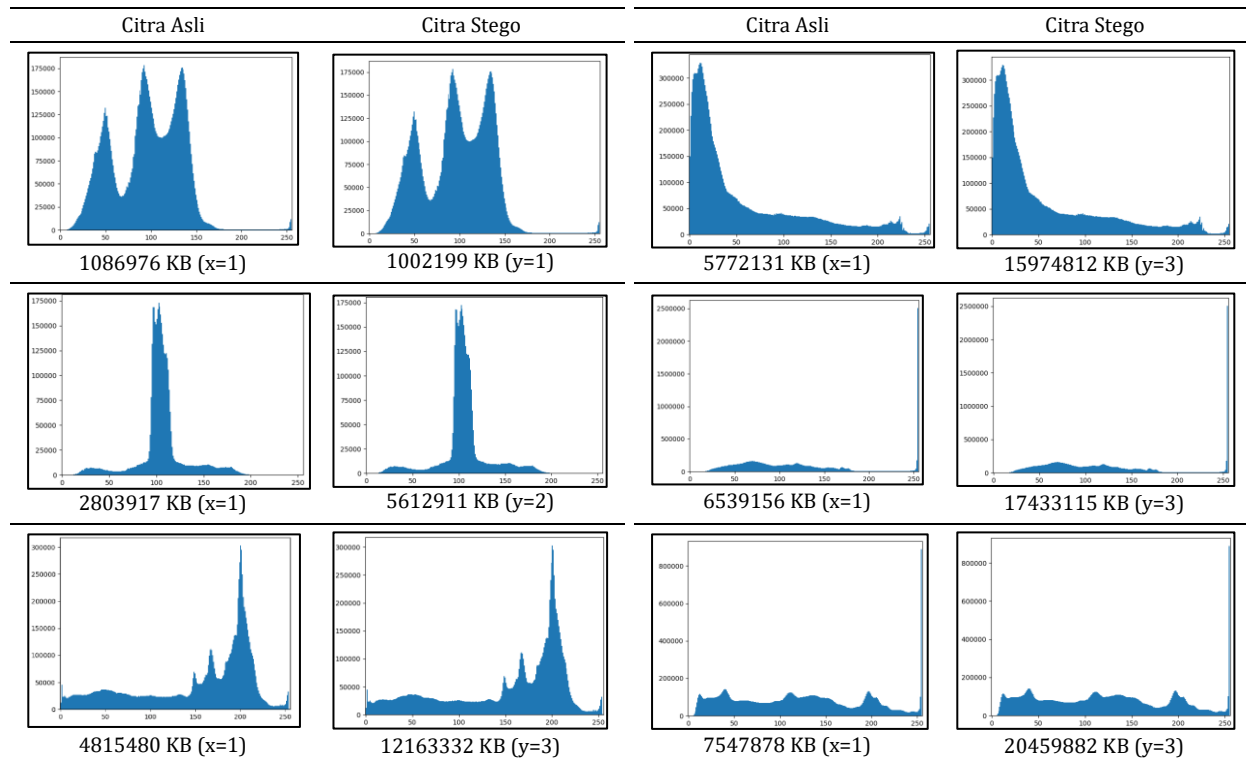
dalam array. Pengamanan informasi pada hasil plainteks dan cipherteks mengalami perbandingan 1:2. Pembuktian lain, jika kapasitas penyisipan informasi dipengaruhi oleh nilai piksel, sehingga ukuran citra yang tinggi penyisipan informasinya lebih banyak. Terbukti jika citra asli dengan kapasitas + 2000000 KB (dalam biner) atau 2MB mampu menampung sekitar informasi 500 karakter.

2. Evaluasi Pixel Histogram Difference

Pengujian ini menggunakan teknik mengevaluasi perbedaan citra Histogram antara citra asli dengan citra stego. Teknik pengujian menggunakan Pixel Histogram Difference (PHD)(Chang & Tai, 2012). Penyisipan informasi dengan ukuran secara bertingkat dari citra asli dengan ukuran 158304-1086976 KB dalam biner disisipi 100 karakter dan citra asli ukuran lebih dari itu disisipi 200 karakter dengan menggunakan kunci yang sama 'Steganografi 2019:*'. Hasil pengujian ditunjukkan pada Tabel 2.

Tabel2. Evaluasi Pixel Histogram Difference












Sumber: (Wati, Sa'diyah, & Ariyus, 2019)






Pada Tabel2. evaluasi histogram histogram citra asli dengan citra stego tidak terlalu nampak perbedaannya. Padahal kedua citra tersebut memiliki ukuran yang berbeda, dimana citra stego cenderung lebih besar dengan perbandingan x:y

yaitu dengan nilai rata-rata 1:4, namun tetap memiliki dimensi yang sama. Sehingga kinerja LSB baik digunakan untuk penyisipan pesan berdasarkan interpretasi Histogramnya

3. Visualisasi Citra melalui Media Komunikasi

Tabel3. Pengujian Visualisasi Citra melalui Media Komunikasi

Via Pengiriman	Citra Asli	Deskripsi Citra Asli			Proses Enkripsi	Deskripsi Stego Citra			Proses Dekripsi
		Tipe	Dimensi (pixels)	Ukuran (KB) Biner		Tipe	Dimensi (Pixels)	Ukuran (KB) Biner	
Telegram		.jpeg	1024 x 640	366168	Berhasil	.png	-	-	Gagal
Telegram		.jpeg	2434 x 1697	2803917	Berhasil	.png	-	-	Gagal
Telegram		.jpeg	1024 x 640	246473	Berhasil	.png	-	-	Gagal
WhatsApp		.jpeg	1024 x 640	366168	Berhasil	.png	-	-	Gagal
WhatsApp		.jpeg	2434 x 1697	2803917	Berhasil	.png	-	-	Gagal
WhatsApp		.jpeg	1024 x 640	246473	Berhasil	.png	-	-	Gagal
Email		.jpeg	1024 x 640	366168	Berhasil	.png	1024 x 640	1026004	Berhasil

Via Pengiriman	Citra Asli	Deskripsi Citra Asli			Proses Enkripsi	Deskripsi Stego Citra			Proses Dekripsi
		Tipe	Dimensi (pixels)	Ukuran (KB) Biner		Tipe	Dimensi (Pixels)	Ukuran (KB) Biner	
Email		.jpeg	2434 x 1697	2803917	Berhasil	.png	2434 x 1697	5745711	Berhasil
Email		.jpeg	1024 x 640	246473	Berhasil	.png	1024 x 640	1244082	Berhasil
Instagram		.jpeg	1024 x 640	366168	Berhasil	.png	-	-	Gagal
Instagram		.jpeg	2434 x 1697	2803917	Berhasil	.png	-	-	Gagal
Instagram		.jpeg	1024 x 640	246473	Berhasil	.png	-	-	Gagal

Sumber: (Wati, Sa'diyah, & Ariyus, 2019)

Pengujian pada Visualisasi Citra (lihat Tabel 3) merupakan pengujian yang dengan membandingkan citra asli dengan stego citra ketika sudah dilakukan proses enkripsi dan dekripsi stego-kripto dengan mengamati perubahan secara kasat mata. Visualisasi dilakukan dengan melakukan beberapa skenario melalui via pengiriman media komunikasi. Citra yang sudah terenkripsi kemudian dikirim dan dilakukan pengembalian ke citra asli agar diketahui informasi yang tersembunyi. Informasi yang disisipi sebanyak 50 karakter. Pengujian ini menghasilkan kinerja dari LSB untuk steganografi, sensitif pada proses pengubahan ukuran citra. Hal tersebut terbukti ketika proses pengiriman dengan Telegram, WA, Instagram tidak dapat dilakukan karena sudah mengubah detail citra. Sehingga merusak informasi rahasia didalamnya. Keberhasilan proses enkripsi dan dekripsi hanya via email. Namun warna dari citra tidak mengalami perubahan.

KESIMPULAN

Kesimpulan dari penelitian ini kinerja dari kriptografi Cipher Block Chaining (CBC) mampu bekerja dengan baik ketika proses enkripsi dan dekripsi mampu memproses macam-macam karakter seperti huruf besar-kecil, angka, spasi dan karakter lainnya. Pengamanan informasi plaintexts dan ciphertexts menghasilkan perbandingan 1:2 untuk jumlah karakter ketika proses enkripsi dan dekripsi. Kinerja metode Least Significant Bit (LSB) mampu menyisipkan informasi sangat dipengaruhi nilai piksel pada media citra digitalnya. Perubahan pada ukuran citra stego cenderung lebih besar dengan rata-rata sebesar perbandingan yaitu 1:4, namun dengan dimensi yang tidak berubah. Namun jika di evaluasi dengan histogram *difference*

perbedaan antara keduanya tidak terlalu nampak. Media komunikasi yang baik untuk pertukaran informasi citra terenkripsi menggunakan email, karena LSB sangat sensitif terhadap kerusakan pada citra, sehingga jika citra sudah mengalami perubahan detailnya maka informasi yang terkandung didalamnya akan rusak.

REFERENSI

- Ariyus, D. (2008). *Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi*. Penerbit Andi.
- Arta, Y. (2017). Implementasi Intrusion Detection System Pada Rule Based System Menggunakan Sniffer Mode Pada Jaringan Lokal. *IT JOURNAL RESEARCH AND DEVELOPMENT*, 2(1), 43. [https://doi.org/10.25299/itjrd.2017.vol2\(1\).979](https://doi.org/10.25299/itjrd.2017.vol2(1).979)
- Azmi, F., & Erika, W. (2017). Analisis Keamanan Data Pada Block Cipher Algoritma Kriptografi Rsa. *CESSJournal Of Computer Engineering, System And Science*, 2(1), 102–104. Retrieved from <http://jurnal.unimed.ac.id/2012/index.php/cess/article/view/4967>
- Cahyadi, T. (2012). Implementasi Steganografi LSB Dengan Enkripsi Vigenere Cipher Pada Citra. *TRANSIENT*, 1(4), 281–288. <https://doi.org/10.22487/j26204118.2018.v1.i2.11221>
- Chang, Y. F., & Tai, W. L. (2012). Histogram-based reversible data hiding based on pixel differences with prediction and sorting. *KSII Transactions on Internet and Information*



- 204